GDPR 관리자와 처리자

성균관대학교 법학전문대학원
김일환

1. 관리자의 책임

I. 관리자의 책임

- **Responsibility of the controller** : 관리자는 처리목적, 범위, 개인의 자유와 권리에 대한 위험과 중대함 등을 고려하여 개인정보 처리가 이 규칙을 준수하는 것을 입증할 수 있는 적절한 기술적, 조직적 조치를 시행하여야 함

- 이러한 조치에는 적절한 정보보호정책의 실행도 포함되어야 함

- **Data protection by design and by default** : 처리목적, 범위, 개인의 자유와 권리에 대한 위험과 중대함 등을 고려하여 관리자는 이 규칙의 요구를 충족하고 정보주체의 권리를 보호하기 위하여 처리수단의 결정시점은 물론 처리 시점에서도 정보보호원칙에 부합하는 익명화와 최소수집 등의 적절한 기술적, 조직적 조치를 시행하여야 함

- 관리자는 기본적으로 구체적인 처리목적을 위한 개인정보만이 처리되기 위한 적절한 기술적, 조직적 조치를 시행하여야 함. 이는 수집되는 정보의 양, 처리범위, 저장기간, 접근가능성에도 적용됨

- 제42조에 따른 인증체계는 이 조항에 따른 관리자의 책임준수를 입증하는 요소로 사용될 수 있음

- **Joint controllers** : 둘 이상의 관리자가 정보처리의 목적과 수단을 함께 결정하는 경우 이들은 함(공)동 관리자로서 정보주체의 권리행사와 그들의 의무 등과 관련하여 이 규칙에 따른 의무준수의 책임을 투명한 방법으로 결정해야 함

- 유럽연합 내 상주하지 않는 관리자나 처리자의 대표 :제3조 제2항에 규정된 상황에서, 관리자나 처리자는 유럽연합 내 대표를 서면으로 지정하여야 함
- 이러한 의무는 a) 일시적 처리, 제9조 제1항에서 행해지는 특별한 범주의 정보처리나 제10조 제1항에서 언급된 형사기소에 관한 개인정보를 포함하지 않는 처리, 처리의 성질이나 상황, 범위, 목적을 고려하여 자연인의 자유와 권리에 위험을 초래할 가능성이 없는 처리 b) 공공기관에 의한 처리에는 적용되지 않음

- 대표는 정보주체의 개인정보가 재화 또는 용역의 제공과 관련하여 처리되거나, 그들의 행동이 모니터링되고, 정보주체가 거주하는 회원국 중 한 곳에 임명되어야 함

- 대표는 이 규칙의 준수와 관련하여 개인정보처리에 관한 모든 사항에 관하여 관리자나 처리자로부터 위임 받아야 함

II. 처리자의 책임

- 관리자를 대신하여 처리가 수행되는 경우, 관리자는 해당 처리가 이 규칙의 요구를 충족하고 정보주체의 권리 보호를 확보하기 위한 방법으로 적절한 기술적·조직적 조치와 절차를 시행하기 위한 충분한 보장들을 제공하는 처리자만을 이용하여야 함

- 처리자는 관리자의 구체적이거나 일반적인 사전 승인 없이는 다른 처리자를 고용하지 못함. 일반적 승인의 경우 처리자는 관리자가 처리자의 교체 등에 대하여 반대할 기회 등을 갖도록 알려주어야 함

- 이는 처리자와 관리자 모두를 구속하는 것으로, 처리기간, 처리의 목적과 성격, 개인정보의 유형과 정보주체의 범주, 관리자의 권리와 의무 등을 그 내용으로 하며

- 처리자는 이러한 계약이나 법적 행위에서 특히 개인정보 국외이송을 포함하여 통제자로부터 문서상 지시된 경우에만 개인정보를 처리하며 처리의 본질상 가능한 한, 제3장에 규정된 정보주체의 권리실현 요청에 답변할 관리자의 의무 이행을 위하여, 필요한 기술적·조직적 요건 등을 상세히 규정해야 함

- 관리자를 위하여 구체적인 처리활동을 수행하기 위한 다른 처리자를 원 처리자가 고용하는 경우 원 계약이나 법적 행위에 규정된 동일한 정보보호의무들이 부과되며, 다른 처리자가 이러한 의무를 이행하지 못하는 경우 원 처리자의 책임은 여전히 남아있음

- 관리자와 처리자는 관리자의 지시와 처리자의 의무를 전자적 형태를 포함한 문서로 작성하여야 함

III. 관리자와 처리자의 권한 내 처리

처리자, 그리고 개인정보에 접근하는 관리자 및 처리자의 권한 내에서 활동하는 자는, 유럽연합이나 회원국 법률에 의하여 요구되지 않는 한, 관리자의 지시 이외의 처리를 할 수 없음

IV. 처리활동의 기록

각 관리자와 관리자의 대표는 자신의 책임 하에 처리활동(행위)기록을 보관하여야 함

- 문서에는 최소한 다음의 정보가 포함되어야 함 :

관리자, 또는 공동 관리자 및 관리자 대표, 정보보호 담당자의 성명 및 상세 연락처, 처리목적,
정보주체 및 개인정보의 종류 설명
개인정보의 수령인 또는 수령인의 종류
제3국 또는 국제기구로의 전송의 경우 적절한 안전책의 문서화 등

각 처리자와 처리자의 대표는 관리자를 위하여 수행된 모든 처리활동종류의 기록을 보관하여야 함

- 문서에는 최소한 다음의 정보가 포함되어야 함 :
처리자, 처리자들, 처리가 행해진 각 관리자와 관리자나 처리자의 대표, 정보보호 담당자의 성명 및 상세 연락처
각 관리자를 위하여 수행된 처리종류
제3국 또는 국제기구로의 전송
가능한 경우 제32조 제1항에서 언급된 기술적, 조직적 보안조치들
- 이러한 기록은 전자적 형태를 포함한 문서로 작성하여야 함
- 관리자나, 처리자, 그 대표는 감독기관이 요구하는 경우 이러한 기록을 이용할 수 있도록 해야 함
- 이러한 기록의무는 제9조 제1항에서 언급된 특별한 범주의 정보처리나 제10조에서 언급된 형사기소에 관한 개인정보처리나 처리의 성질이나 상황, 범위, 목적를 고려하여 자연인의 자유와 권리에 위험을 초래할 가능성이 있는 처리나 일시적이지 아니한 처리가 아닌 한, 250명 이하를 고용하는 기업이나 조직에는 적용되지 않음

V. 감독기관과의 협력

관리자와 처리자, 그리고 관리자의 대표가 존재하는 경우 그 대표는 그 의무를 수행함에 있어 감독기관의 요청에 따라 감독기관과 협력하여야 함

VI. 우리법제

제26조(업무위탁에 따른 개인정보의 처리 제한)
제28조(개인정보취급자에 대한 감독)
제30조(개인정보 처리방침의 수립 및 공개)
제31조(개인정보 보호책임자의 지정)

2. 정보보안

I. 처리보안

1. **필요성:** 관리자와 처리자는 최고(신)기술, 이행비용, 처리목적, 범위, 상황, 개인의 자유와 권리에 대한 위험과 중대함 등을 고려하여 일정한 보안단계를 보장하기 위한 다음과 같은 적절한 기술적, 조직적 조치들을 시행하여야 함 :

2. 개인정보의 익명화와 암호화

- 개인정보처리 시스템과 서비스의 비밀성, 완전성, 복원, 이용가능성
물리적이거나 기술적인 사고가 발생한 경우 시기 적절한 방법으로 개인정보에 접근하고 이용할 가능성을 복원할 능력
처리보안의 확보를 위한 기술적, 조직적 조치들의 효율성을 정기적으로 평가하고 심사하기 위한 절차

- 적절한 보안수준을 평가할 때 관리자와 처리자는, 특히 개인정보의 우연적 또는 불법적 파괴, 도난, 권한 없는 공개 등에서 발생하는 정보처리의 위험 등을 고려해야 함

3. 우리법제

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. <개정 2015.7.24.>

정보통신망법 제28조(개인정보의 보호조치)

① 정보통신서비스 제공자 등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다. <개정 2016.3.22.>

② 정보통신서비스 제공자 등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다. <개정 2016.3.22.>

[전문개정 2008.6.13.]

II. 감독기관에 개인정보 침해 통지

- 개인정보 침해가 발생한 경우, 개인정보침해가 자연인의 자유와 권리에 위험을 야기할 가능성이 없는 게 아닌 한, 관리자는 그 사실을 인지한 후 72시간 내에 지체 없이 해당 침해 사실을 감독기관에 통지하여야 함

- 감독기관에의 통지가 72시간 내에 이루어지지 않은 경우 이를 정당화할 사유를 함께 첨부하여 제출하여야 함

- 처리자는 개인정보침해가 성립한 후 관리자에게 이를 즉시 알려야 함
- 위 통지에는 정보주체의 분류와 수, 그리고 문제가 된 정보기록의 종류와 수를 포함한 개인정보 침해의 내용 설명 정보보호 담당관 또는 정보를 제공받을 수 있는 다른 연락 창구의 신원 및 세부 연락처, 개인정보침해의 결과 설명, 개인정보침해에 대하여 관리자가 취했거나 계획중인 조치들의 설명이 있음
- 관리자는 개인정보침해와 관련된 사실, 효과 및 구제 조치 등을 포함한 개인정보 침해 내용을 문서화하여야 함
- 감독기관은 이 문서로 이 조항의 준수여부를 검증할 수 있어야 함

III. 정보주체에 개인정보침해 통지(communication)

- 개인정보침해가 정보주체의 자유와 권리침해에 대한 위험이 높은 경우, 관리자는 지체 없이 정보주체에게 개인정보침해를 알려야 함

- 정보주체에게 통지는 분명하고 쉬운 용어로 개인정보침해의 성격, 정보주체의 분류와 수, 그리고 문제가 된 정보기록의 종류와 수를 포함한 개인정보 침해의 내용, 정보보호 담당관 또는 정보를 제공받을 수 있는 다른 연락 창구의 신원 및 세부 연락처를 알려주어야 함

- 관리자가 자신이 적절한 기술적 보호 조치를 취하였고, 정보주체의 자유와 권리에 대한 높은 위험성이 구체화되지 않도록 보장하는 후속조치들을 취하였고, 너무 과한 노력을 수반하는(그러한 경우 정보주체에게 똑같은 효율적 방법으로 통지되는 공적 통지나 유사한 조치들) 조건을 충족하는 경우에는 정보주체에게 개인정보 의무위반을 통지할 필요가 없음
- 관리자가 개인정보침해를 정보주체에게 알리지 않은 경우, 감독기관은 해당 침해의 부정적 영향 가능성을 고려하여 관리자의 개인정보 침해 통지 의무를 해하지 않고 그러한 통지를 하도록 요청할 수 있음

IV. 우리 법제

제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다

③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정자치부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다 <개정 2013.3.23., 2014.11.19.>

④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다

3. 정보 보호 영향 평가 및 사전 승인

I. 정보보호 영향평가

- 특히 새로운 기술을 사용하고, 처리의 성격, 범위, 상황, 목적을 고려하여 처리의 유형이 개인의 자유와 권리와 자유에 높은 위험을 가져올 수 있다면 관리자는 사전에 개인정보보호에 관한 영향평가를 실시하여야 함

- 관리자는 정보보호 영향평가를 수행하는 경우 정보보호 담당자의 조언을 구해야 함
-
- 정보보호 영향평가는 특히 프로파일링을 포함한 자동화된 처리, 그리고 개인에게 법적 효과를 유발하거나 중대한 영향을 미치는 조치에 근거한 것으로써, 자연인과 관련한 개인적 사항의 체계적이고 광범위한 평가, 인종 또는 민족적 연원, 정치적 견해, 종교나 철학적 신념, 노동조합원, 유전자정보, 자연인 식별목적의 생체정보, 자연인의 성생활 그리고 성적 취향 정보나 건강정보 , 제10조에서 언급된 형사기소 관련 개인정보처리 공적으로 접근 가능한 영역에서 대규모로 행해지는 체계적인 모니터링 경우에는 시행되어야 함

- 감독기관은 정보처리 영향평가에 따라야 할 처리작용의 목록을 작성하고 공포할 수 있음

- 감독기관은 또한 정보처리 영향평가가 요구되지 않는 처리작용의 목록을 작성하고 공포할 수 있음

- 평가에는, 관리자의 정당한 이익을 포함한 처리목적, 예상되는 처리작용의 체계적 설명 처리목적과 관련되는 처리작용의 필요성과 비례성 평가 ,정보주체의 자유와 권리에 대한 위험평가, 정보주체와 관련 당사자들의 권리와 정당한 이익을 고려하여 이 규칙에 부합하고 개인정보 보호를 확보하는 보호장치와 대책들을 포함한 조치들을 담고 있어야 함

II. 사전 자문

- 관리자의 조치가 없는 경우 정보처리가 높은 위험을 야기할 가능성이 있음을 정보보호영향평가가 지적하는 곳에서 관리자는 감독기관에 사전 자문을 얻어야 함

- 계획된 처리가 이 규칙에 부합되지 않는다고 감독기관이 판단한 경우 최대 8주 내에 정보관리자에게 권고를 해야 함. 이러한 기간은 계획된 처리의 복잡성을 고려하여 6주 더 연장될 수 있음

- 이러한 기간의 경과는 자문목적으로 감독기관이 요구하는 정보를 획득할 때까지 정지됨

- 감독기관의 자문 시 관리자는 감독기관에게 관리자, 공동 관리자, 처리자 각각의 책임 계획된 처리의 목적과 방법들이 규칙에 따라 정보를 제공해야 함

- 회원국은 계획된 처리에 관한 입법적 조치를 위한 제안준비단계에서 감독기관의 자문을 얻어야 함

III. 우리 법제

제8조의2(개인정보 침해요인 평가) ① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다

② 보호위원회가 제1항에 따른 요청을 받은 때에는 해당 법령의 개인정보 침해요인을 분석·검토하여 그 법령의 소관기관의 장에게 그 개선을 위하여 필요한 사항을 권고할 수 있다

③ 제1항에 따른 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항은 대통령령으로 정한다

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 행정자치부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정자치부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다

② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다
1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항
③ 행정자치부장관은 제1항에 따라 제출 받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다
④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조 제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다
⑤ 행정자치부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다
⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다
⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다
⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다

3. 정보보호 담당관

I. 정보보호 담당관의 지정

- 관리자와 처리자는 법원을 제외한 공공기관이 수행하는 처리의 본질, 범위 및 목적에 따라 관리자 또는 처리자의 핵심활동이 정보주체의 정기적·체계적 모니터링을 요구하는 처리,제9조에 따른 특별한 정보항목을 대규모로 처리하는 경우와 와 제10조에 규정된 형사기소 관련 개인정보를 처리하는 경우 정보보호 담당관을 지정하여야 함

- 공공기관이 관리자 또는 처리자인 경우, 그들의 조직과 구조와 규모를 고려하여 여러 기관을 위한 1명의 정보보호 담당관을 지정할 수 있음

- 제1항에 규정된 경우를 제외하고, 관리자 및 처리자, 또는 협회 그리고 그 밖에 관리자 및 처리자의 분류를 대표하는 기관들은 정보보호 담당관을 지정할 수 있음

- 정보보호담당관은 전문적 자질, 특히, 정보보호 법령과 실무에 대한 전문 지식과 제37조에 규정된 임무를 수행할 수 있는 능력을 보유한 자이어야 함, 관리자 또는 처리자는 정보보호 담당관의 성명과 세부 연락처를 감독기관에 통지하고 공개하여야 함

II. 정보보호 담당관의 지위

- 관리자 또는 처리자는 정보보호담당관이 개인정보의 보호와 관련된 모든 문제에 적절하고 신속한 방법으로 관여할 것을 보장하여야 함

- 관리자 또는 처리자는 정보보호 담당관에게 그들의 전문지식을 유지하고, 개인정보처리활동에 접근하고 그들의 임무수행을 위하여 필요한 자료들을 제공하여 제39조에 규정된 임무 수행 시 정보보호 담당관을 지원해야 함

- 관리자 또는 처리자는 담당관 임무행사 시 어떤 지시를 받지 않도록 보장하고, 담당관은 임무수행과 관련하여 징계나 해고되지 않아야 하며, 최고위층 관리자나 처리자에게 직접 보고하여야 함

- 정보주체는 개인정보처리 관련 모든 문제 및 이 규칙에 따른 자신의 권리행사에 관하여 정보보호담당관과 접촉할 수 있음

- 정보보호담당관은 유럽연합이나 회원국 법률에 따른 비밀유지의무 하에 있음

III. 정보보호 담당관의 의무

- 정보보호 담당관은 최소한 이 규칙과 유럽연합 및 회원국 정보보호규정들에 따른 그들의 의무를

- 관리자와 처리자 및 직원에게 통지하고 자문하고,

- 이 규칙과 유럽연합 및 회원국 정보보호규정들 그리고 개인정보보호와 관련한 관리자 및 처리자의 정책준수의 모니터링 정보보호영향평가관련 자문 그리고 제35조에 따른 모니터링, 감독기관과 협조, 개인정보처리 관련 문제에서는 감독기관과 연결통로로 활동할 임무를 가져야만 함

4. 행동 강령 및 인증

I. 행동 강령

- 회원국, 감독기관 및 유럽정보보호위원회는 다양한 정보처리부문, micro-, 소규모, 중간규모의 기업의 구체적 특징을 고려하여 이 규칙의 적절한 적용을 위한 행동강령제정을 촉진하여야 함

- 관리자와 처리자를 위한 협회나 기관들은 공정하고 투명한 정보처리 구체적 상황에서 관리자가 추구하는 정당한 이익, 개인정보수집 개인정보 익명화 공공 등의 이 규칙의 적용을 구체화하는 행동강령을 만들거나 개정할 수 있음

- 행동 강령을 제정 또는 기존 강령의 개정 및 확대를 원하는 회원국 내 협회와 다른 기관들은 회원국 내 감독기관에 그러한 의견을 제출할 수 있으며, 유럽정보보위원회는 행동 강령의 제정안 또는 개정안이 이 규칙에 부합하는지의 여부에 관한 의견을 줄 수 있음

- 유럽정보보호위원회는 모든 승인된 행동강령을 수집하고 적절한 수단들을 통하여 공개될 수 있도록 해야만 함

II. 승인된 행동강령의 모니터(감독)

- 규칙 제57조와 제58조에 따른 감독기관의 권한과 임무를 해지지 않고 제40조에 따른 행동강령 준수 모니터링은 적절한 수준의 전문가기관과 감독기관에 의하여 이러한 목적으로 인정된 기관이 수행할 수 있음

- 이러한 기관은 독립성과 전문성을 입증하고, 모니터링 등 관련 절차를 만들고 행동강령 위반에 대한 이의제기를 다룰 절차와 정보주체와 공중에게 투명한 절차 등을 만들 수 있음

- 이 규정은 공공기관이 수행하는 처리에는 적용되지 않음

III. 인증 및 인증기관과 절차

- 회원국과 감독기관, 유럽정보보호위원회와 유럽위원회는, 특히 유럽 차원에서, 관리자 및 처리자가 수행하는 정보처리가 이 규칙에 부합하는지를 입증하기 위한 목적으로 정보보호 인증 체계와 씰 및 마크의 도입을 촉진하여야 함
- 소규모, 중간규모의 기업의 구체적 요구(필요)는 고려해야 함
- 인증은 자발적이고 투명한 절차에 의하여 이용할 수 있어야 함
- -이 조항에 따른 인증은 이 규칙을 준수할 관리자나 처리자의 책임을 축소하지 않으며 감독기관의 과제와 임무에 영향을 주지 않음
- 이 조항의 인증은 적절한 인증기관이나 권한 있는 감독기관 등이 할 수 있음
- 관리자나 처리자는 인증을 위하여 필요한 모든 정보나 처리활동에 접근을 적절한 인증기관이나 권한 있는 감독기관에 제공해야 함

- 인증은 최대 3년간 유효하며 요구조건을 충족하지 못하면 철회됨
- 유럽정보보호위원회는 모든 인증체계를 수집하고 적절한 수단들을 통하여 공개될 수 있도록 해야만 함

IV. 우리법제

제32조의2(개인정보 보호 인증)

① 행정자치부장관은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다
② 제1항에 따른 인증의 유효기간은 3년으로 한다
③ 행정자치부장관은 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다
1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우
2. 제4항에 따른 사후관리를 거부 또는 방해한 경우
3. 제8항에 따른 인증기준에 미달하게 된 경우
4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우
④ 행정자치부장관은 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다

IV. 우리법제

⑤ 행정자치부장관은 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제3항에 따른 인증 취소, 제4항에 따른 사후관리 및 제7항에 따른 인증 심사원 관리 업무를 수행하게 할 수 있다
⑥ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다
⑦ 제1항에 따른 인증을 위하여 필요한 심사를 수행할 심사원의 자격 및 자격 취소 요건 등에 관하여는 전문성과 경력 및 그 밖에 필요한 사항을 고려하여 대통령령으로 정한다
⑧ 그 밖에 개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합하는지 여부 등 제1항에 따른 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다

Thank YOU!